



## HIPAA Checklist for Facilities

### Final Rules for Transactions, Code Sets and Privacy

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 includes provisions for the simplification of administrative and financial health care transactions by standardizing the electronic exchange of information between health care plans, clearinghouses and providers. These standards are described in two final rules: Standards for Electronic Transactions and Code Sets with a compliance date of October 16, 2002 and Privacy with a compliance date of April 14, 2003.

Please have your Information Technology (IT) staff complete the checklist below and analyze the results to determine your facility's technical readiness. This tool will bring HIPAA to the attention of the facility, staff and management. The checklist and results are for your use only and will not be collected by the Department of Health Services (DHS). This is not an official technical assessment for HIPAA compliance.

<b>Workstations</b>	<b>Yes</b>	<b>No</b>
Do you keep an inventory of your workstations?	<input type="checkbox"/>	<input type="checkbox"/>
Does each staff member work at his or her own workstations?	<input type="checkbox"/>	<input type="checkbox"/>
Are your workstations locked and secure?	<input type="checkbox"/>	<input type="checkbox"/>
Is staff allowed to bring devices from home to attach to the workstations?	<input type="checkbox"/>	<input type="checkbox"/>
Are the floppy drives enabled?	<input type="checkbox"/>	<input type="checkbox"/>
Do you use zip drives or read/write CD ROMs to download data?	<input type="checkbox"/>	<input type="checkbox"/>
Do you use password protection?	<input type="checkbox"/>	<input type="checkbox"/>
Who troubleshoots your computer workstations?		
Do you track the warranties on the workstations?	<input type="checkbox"/>	<input type="checkbox"/>
<b>Server Hardware</b>	<b>Yes</b>	<b>No</b>
How many servers do you have onsite?		
Does each remote site have its own server?	<input type="checkbox"/>	<input type="checkbox"/>
Are the servers kept in a locked area?	<input type="checkbox"/>	<input type="checkbox"/>
Are the servers kept in a well-ventilated area?	<input type="checkbox"/>	<input type="checkbox"/>
Are the servers in an area that has flooded?	<input type="checkbox"/>	<input type="checkbox"/>
Do the servers have an Emergency Power Supply (EPS)?	<input type="checkbox"/>	<input type="checkbox"/>
Who handles the maintenance on the servers?		
Do the servers have backup capability and hardware?	<input type="checkbox"/>	<input type="checkbox"/>
Do you do a backup of information on the servers?	<input type="checkbox"/>	<input type="checkbox"/>
How often do you perform a backup on the servers?		
Who handles the backup?		
Are the backups stored off-site?	<input type="checkbox"/>	<input type="checkbox"/>
Who handles recovery from a backup?		
Who handles technical problems on your servers?		
Do you track the warranties on the servers?	<input type="checkbox"/>	<input type="checkbox"/>
<b>SOFTWARE</b>	<b>Yes</b>	<b>No</b>
<b>Clinic Management Software</b>		
Are there passwords to access the clinic management software?	<input type="checkbox"/>	<input type="checkbox"/>
Are there different levels of security?	<input type="checkbox"/>	<input type="checkbox"/>
Are there auditing features?	<input type="checkbox"/>	<input type="checkbox"/>
At what level do they audit? User? Information?		
Is downloaded information secure?	<input type="checkbox"/>	<input type="checkbox"/>
Are there procedures to handle sensitive information, for example, HIV patients?	<input type="checkbox"/>	<input type="checkbox"/>
Is a password required to enter the database?	<input type="checkbox"/>	<input type="checkbox"/>
Is a password required to view the security files?	<input type="checkbox"/>	<input type="checkbox"/>
Is terminal emulation used with the system?	<input type="checkbox"/>	<input type="checkbox"/>
Who handles problems and issues with the clinic management software?		

<b>PC Software</b>	<b>Yes</b>	<b>No</b>
Are any PC applications integrated with the clinic management software?	<input type="checkbox"/>	<input type="checkbox"/>
Are all software applications licensed?	<input type="checkbox"/>	<input type="checkbox"/>
Who loads the PC applications onto the PC?		
Is there a standard PC package?	<input type="checkbox"/>	<input type="checkbox"/>
<b>Networks</b>	<b>Yes</b>	<b>No</b>
Do you operate a Local Area Network (LAN)?	<input type="checkbox"/>	<input type="checkbox"/>
Do you operate a Wide Area Network (WAN)?	<input type="checkbox"/>	<input type="checkbox"/>
Does your network interface with the Internet?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have an Internet firewall?	<input type="checkbox"/>	<input type="checkbox"/>
Is network access governed by passwords?	<input type="checkbox"/>	<input type="checkbox"/>
Are there various levels of security?	<input type="checkbox"/>	<input type="checkbox"/>
Who has supervisor access?		
Is the network used for file sharing?	<input type="checkbox"/>	<input type="checkbox"/>
<b>Security</b>	<b>Yes</b>	<b>No</b>
Are passwords changed on a regular basis?	<input type="checkbox"/>	<input type="checkbox"/>
Are temporary passwords assigned to non-permanent employees?	<input type="checkbox"/>	<input type="checkbox"/>
Are the user lists audited against the current lists of employees?	<input type="checkbox"/>	<input type="checkbox"/>
Is dial-in access allowed?	<input type="checkbox"/>	<input type="checkbox"/>
If so, who has dial-in access?	<input type="checkbox"/>	<input type="checkbox"/>
<b>Telemedicine</b>	<b>Yes</b>	<b>No</b>
Does your clinic provide telemedicine services?	<input type="checkbox"/>	<input type="checkbox"/>
Are these services provided in private residences?	<input type="checkbox"/>	<input type="checkbox"/>
<b>Data Transfer</b>	<b>Yes</b>	<b>No</b>
Does your clinic engage in any electronic data transfers?	<input type="checkbox"/>	<input type="checkbox"/>
Do you use a third-party data clearinghouse to transfer information?	<input type="checkbox"/>	<input type="checkbox"/>
Who are your electronic data interchange (EDI) vendors?		
Do you ever use floppy disks for data transfer?	<input type="checkbox"/>	<input type="checkbox"/>
Do you ever send data transfers via e-mail?	<input type="checkbox"/>	<input type="checkbox"/>
Do you ever send data transfers via the Internet?	<input type="checkbox"/>	<input type="checkbox"/>
What transfer file format do your vendors require?		
What is the delimiter of your database?		
<b>Medical Records</b>	<b>Yes</b>	<b>No</b>
Are your medical records stored electronically?	<input type="checkbox"/>	<input type="checkbox"/>
Do you ever fax your medical records to other sites?	<input type="checkbox"/>	<input type="checkbox"/>
Are your medical records regularly audited?	<input type="checkbox"/>	<input type="checkbox"/>
Are your medical records stored in a secure area?	<input type="checkbox"/>	<input type="checkbox"/>
Do you use an outside transcription service?	<input type="checkbox"/>	<input type="checkbox"/>

This checklist is to be used only as a tool to assist facilities in HIPAA awareness. It is the responsibility of every facility to assess and comply with the HIPAA mandates. Medi-Cal, the State of California and EDS are not responsible for providers becoming HIPAA compliant.